Exhibit 2

Issue Notification

Third-Party Security and Privacy Risk

First notification: April 10, 2024

For more information about Security and Privacy Vulnerability escalations, refer to the Escalation Process for Potential Security and Privacy Issues in Epic Software document on Galaxy.

Summary

We have identified a third-party privacy risk that might affect your organization. Please read this document closely and work with your Epic Technical Services representative to determine if you are affected by this issue and to identify an appropriate resolution plan.

Title	Potentially Inappropriate Disclosures of Protected Health Information Through the Carequality Interoperability Framework
Issue ID	Q-7475908
Applications	Care Everywhere
Versions	All versions
Availability	Actual

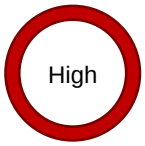
Exploitability	Impact
	

Table of Contents

Description

Summary

The Carequality interoperability framework was founded based on the Carequality Principles of Trust, which include core principles such as HIPAA Compliance, Non-Discrimination, Cooperation, Acceptable Use, and Accountability. This framework relies on those principles being followed to establish interoperability at a national level without needing to have individual contracts or technical connections among agreeing parties.

This Third-Party Security and Privacy Risk Notification outlines events that have led Epic to file a formal dispute with Carequality over serious concerns about security and privacy arising from activities of a third-party participant implementer in Carequality (Particle Health), including:

- loading significant volumes of Particle Health participants to the point of causing the Carequality directory infrastructure to become non-responsive;
- significant patient record exchange pattern anomalies including batches of large numbers of records being requested in a certain geographical region;
- a pattern of only one-way data exchange from Epic customer organizations without reciprocal data exchange from the Particle Health's connections, which suggests a non-treatment use case despite Particle Health's representations of a Treatment Permitted Use;
- demonstrating a pattern of a lack of transparency, including obscuring provider-level details of connections through a generic gateway and declining to provide full information requested about their connections over the course of several months; and
- failing to timely remove hundreds of directory entries after more than 30 Epic customer organizations objected to their purported "on behalf of" relationship with the Particle Health participants.

Epic Carequality Administrators and members of the Epic community's Care Everywhere Governing Council reviewed Particle Health participants' use cases and determined that certain Particle Health participants may not be eligible to assert a Treatment Permitted Purpose. At the Care Everywhere Governing Council's recommendation, due to the significant security and privacy concerns, on March 21, 2024, Epic filed a formal dispute with Carequality on the grounds that Particle Health might not be fulfilling its obligations as a Carequality implementer, and based on the concern that Particle Health and its participant organizations might be inaccurately representing the purpose associated with their record retrievals. This poses potential security and privacy risks, including the potential for HIPAA Privacy Rule violations in the event disclosures of protected health information were made under the Treatment Permitted Purpose when the requesting entities did not have treatment relationships with the patients to whom the records related.

While the Carequality dispute is in progress and the ongoing potential for risks remains high, pursuant to the Epic Carequality Phonebook Support Policy, Epic Carequality Administrators suspended Particle Health's generic gateway connection on March 21 as Epic and the Care Everywhere Governing Council were unable to verify a Treatment Permitted Purpose.

Prior to the suspension of Particle Health's generic gateway, Particle Health and its participant organizations had requested and received hundreds of thousands of electronic health records from Epic customer community members that participate in Carequality. Some number of those record retrievals might have inaccurately claimed Treatment as the Permitted Purpose.

Issue Details

Background

Carequality is a nationwide interoperability framework that supports several Permitted Purposes*. It is made up of dozens of implementer organizations that in turn onboard their participant organizations to the framework. Implementers identify their participants' Permitted Purposes when they join the framework.

Under the Carequality Framework, a "Permitted Purpose" is a defined set of reasons for which a request for electronic health records can be performed. Each request for an individual's record contains the Permitted Purpose as part of the technical transaction making the request for information.

Epic implements connectivity to Carequality as an extension of its Care Everywhere network. Accordingly, Epic supports a purpose-built set of Permitted Purposes through Carequality. All of Epic's clinical customers that are eligible for Carequality participate and will respond to the Treatment** Permitted Purpose. The Epic Carequality Administrators review all new participant connections under the Epic Carequality Phonebook Support policy prior to establishing their connections with the Epic community. Organizations that wish to exchange information with Epic customer community members for purposes other than treatment can do so through a number of other pathways, including USCDI APIs, additional FHIR APIs, automated CDA extracts, HL7 interfaces, and the EHI Export tool, the specifications and endpoints for which Epic publishes online at open.epic.com.

The Carequality framework policies require that organizations claiming Treatment as the Permitted Purpose must be providing treatment or be making requests for health information on behalf of a network member that is providing treatment to the individual who is the subject of the requested records.

Particle Health, an implementer on the Carequality interoperability framework, has connected participant organizations to the Carequality framework with a Permitted Purpose of Treatment. All of Particle Health's participant organizations claimed a Permitted Purpose of Treatment when requesting and retrieving records from Epic Carequality participants.

Particle Health has a centralized gateway that processes all their participant organization's connectivity to Carequality, meaning that exchanges of electronic health records with Particle Health's participant organizations pass through the Particle Health gateway as opposed to a federated system where trading partners exchange directly with each other.

*See the full list of Permitted Purposes in section 3.1 of the Carequality Query-Based Document Exchange Implementation Guide.

**As defined at 45 C.F.R. 164.501 (*See* https://www.ecfr.gov/current/title-45/part-164/section-164.501#p-164.501(Treatment).

Timeline

Starting in October 2023, Particle Health published thousands of new participant connections to Carequality under the Permitted Purpose of Treatment. As provided by the Epic Carequality Phonebook Support Policy, Epic Carequality administrators reviewed these entries to determine whether they were appropriate to connect under the Treatment Permitted Purpose and flagged them for further review with the Epic community's Care Everywhere Governing Council. That Governing Council is comprised of 15 representatives elected from Care Everywhere participant organizations and is tasked with providing oversight for the Care Everywhere network and compliance with the Care Everywhere Rules of the Road. The Governing Council determined that the Particle Health entries for MDPortals, Reveleer, and Integritort likely did not conform to a Treatment Permitted Purpose and directed Epic to not connect those participant entries to the Epic community.

Over the course of several months between October 2023 and April 2024, Particle Health, Epic, and Carequality had multiple conversations related to processing new entries and Particle Health's implementer obligations.

Additionally, many of Particle Health's new directory entries asserted relationships with Epic community members to allow those entries to make treatment requests on their behalf, known as "On Behalf Of" (OBO) in the Carequality Framework

Policies. Every Epic community member that reviewed these relationships dating back to December 2023 objected to them. As indicated by the Carequality framework policies in 3.2.1.3:

> "*If an OBO entry's referenced organization objects in any way to that relationship, the OBO entry MUST remove the reference to that [Carequality Connection] or suspend their use of Carequality until the responding organization has confirmed the relationship with Carequality*."

In March 2024, Epic Carequality administrators became aware of a significant increase in the volume of records sent from Epic organizations directly to the Particle Health gateway entry between November 2023 to December 2023. This increase coincided with Particle Health's additions of MDPortals, Reveleer, and Integritort to the Carequality directory, which based on the Care Everywhere Governing Council's direction had not yet been distributed to the Care Everywhere network. Epic also learned that another implementer planned to file a formal dispute with Carequality alleging that Integritort used the Carequality framework to obtain health information for the apparent purpose of identifying potential participants in class action lawsuits while claiming a Permitted Purpose of Treatment.

After consideration of the information known at the time, the Care Everywhere Governing Council directed Epic to file a formal dispute with Carequality as provided in the Carequality framework agreement, and to suspend Particle Health's gateway connection to Epic community members while the Carequality dispute is pending. On March 21, Epic filed a formal dispute with Carequality, and Epic Carequality Administrators suspended Particle Health's gateway connection to Epic community members.

On March 22, Particle Health's Integritort Carequality directory entry was marked inactive in the Carequality directory by either Particle Health or Integritort. No information to date has been shared with the Carequality community about why this was marked inactive.

On March 28, the Epic Carequality Administrators became aware of another Particle Health participant, Novellia, claiming a Treatment Permitted Purpose while describing their product publicly as a personal health tool. The Care Everywhere Governing Council determined that Novellia's activities did not conform to a Treatment Permitted Purpose and directed Epic to not distribute Novellia's connection to the Epic community, and Epic Carequality Administrators did not do so.

After further review of Particle Health's participant connections and to safeguard the privacy of patients across the Epic community, the Care Everywhere Governing Council determined that for connectivity to remain active, Epic should require Particle Health to supply additional information to support each of their participants' Treatment Permitted Purposes.

On April 4, Epic requested that Particle Health provide sufficient information necessary to complete the verification of the Treatment Permitted Purposes.

On April 8, Carequality staff convened a pre-dispute panel meeting with Epic and Particle Health representatives to further discuss the dispute details and information Epic requested to complete the verification of Treatment Permitted Purposes for Particle Health's participants. Epic has requested that Carequality expedite its dispute process to address these concerns. In the meantime, Epic is actively working with Particle Health to determine whether any of its connections previously associated with their generic gateway are for the Treatment Permitted Purpose and, if appropriate, to establish those connections.

On April 9, the Care Everywhere Governing Council met to discuss the new Particle Health participants that Particle Health identified as previously behind the generic Particle Health gateway. Multiple members of the council questioned Carequality's role in overseeing and vetting new entries being onboarded to their framework, and some also objected to relationships purported by Particle Health's participants with their representative organizations. They were unable to verify any additional connections should be established at this time. The Governing Council asked Epic to seek additional information about these participants prior to distributing new entries to the Care Everywhere network.

On April 10, Epic and Particle Health again participated in a pre-dispute panel meeting to discuss the dispute and to discuss a plan for verifying certain participants were exchanging records for a Treatment Permitted Purpose and to establish those connections. Epic again requested that Carequality move quickly to convene a dispute panel which as of today, has not been established.

Investigation Steps

All electronic health records your organization might have disclosed to Particle Health through its gateway and to its participants were requested under a Treatment Permitted Purpose. There is no programmatic way to determine whether those requests were appropriately made under a Treatment Permitted Purpose.

A search is available to determine the number of patients with records retrieved by Particle Health participant organizations and by the generic Particle Health gateway. With treatment-related record exchanges, it is typical to see a steady flow of data both sent and received as patients are treated by multiple providers. A high number of records sent with a low number of records received is atypical of record exchange patterns for the purpose of treatment and might suggest a non-treatment purpose.

To help you prioritize your investigation, the search results include the ratio of successful patient queries your organization made to Particle Health participants regarding patients whose records were retrieved from you by a Particle Health participant. The Particle Health gateway will be included as an individual entry in the search results.

Contact your Care Everywhere Epic representative and mention SLG 8714758 for help understanding the search results for your investigation.

To investigate individual record releases to the identified organizations, you can use the HIM Disclosures Report. Add a criterion for the CE Organization ID (I ROI 300) item to search based on the Organization (DXO) ID provided in the search results referenced above. Contact your HIM Epic representative and mention SLG 8714758 if you need help running this report.

If, during your investigation, you have questions about any of the record retrievals made by Particle Health or one of its participant organizations, contact Particle Health at support@particlehealth.com.

If you have any additional information to indicate that a Particle Health participant does or does not conform to a Treatment Permitted Purpose, contact the Epic Carequality Administrators at CarequalityAdmins@epic.com.

Resolution

Special Updates

Because this risk does not exist in Epic software, special updates will not be released to resolve this issue.

Mitigating Risk

Should any additional actions need to be taken to further mitigate security and privacy risks from this issue, Particle Health's participant connections may be deactivated on behalf of the Epic community. All Particle Health participants that are deactivated will no longer be able to retrieve records from Epic organizations through Particle Health's gateway; similarly, Epic organizations will no longer be able to retrieve records from deactivated Particle Health participants. Previously retrieved records will still be available. Participant connections can be reinstated on a case-by-case basis.

Organizations that wish to exchange information with Epic customer community members for purposes other than treatment can do so through a number of other pathways, including USCDI APIs, additional FHIR APIs, automated CDA extracts, HL7 interfaces, and the EHI Export tool, the specifications and endpoints for which Epic publishes online at open.epic.com.

If you have any additional information to indicate that a Particle Health participant does or does not conform to a Treatment Permitted Purpose, contact CarequalityAdmins@epic.com.

As a general best practice, monitoring system-level exchange metrics can help detect unusual record exchange patterns. More detailed follow-up can then be made with outside entities with which unusual exchange patterns are detected. Tools are available in Epic to monitor exchange rates over time, compare outgoing versus incoming record volumes with individual organizations, and track significant changes in the number of records sent to those organizations.

Refer to the Monitor Exchange Discrepancies Based on the Ratio of Patient Records Exchanged and Monitor Exchange Discrepancies Based on Volume of Patient Records Sent topics on galaxy for additional details.